

Amendments to the Claims:

1. (Previously Presented) A method for providing network security, comprising the steps of:

receiving a plurality of network protocol packets, wherein a network protocol packet includes a network protocol header and a plurality of network protocol data, and wherein the network protocol data include a first cryptographic protocol header and a first plurality of encrypted data, at least a portion of at least some of the network protocol packets being configured in accordance with a transport layer protocol or a network layer protocol;

determining a first plurality of cryptographic protocol rules associated with the network protocol data;

establishing a cryptographic session, if required by said first cryptographic rules;

applying the first plurality of cryptographic protocol rules to the first encrypted data to obtain a first plurality of cleartext data;

translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule; and

encrypting the second plurality of cleartext data in accordance with at least one rule associated with a second cryptographic protocol, resulting in a second plurality of encrypted data.

2. (Previously Presented) A system for providing network security, comprising:

an input module for receiving a plurality of network protocol packets, at least a portion of at least some of the network protocol packets being configured in accordance with a transport layer protocol or a network layer protocol;

a translation module for translating a first plurality of data into a second plurality of data;

an output module; and

a cryptographic module responsive to the input module and the output module for performing cryptographic operations.

3. (Currently Amended) A system for providing network security, comprising;
means for receiving a request to perform a cryptographic operation;
means for returning a response to the cryptographic operation request;
means for translating a first plurality of cleartext data into a second plurality of
cleartext data in accordance with at least one translation rule; and
at least one module for performing said cryptographic operations, said
cryptographic operations including obtaining the first plurality of cleartext data based upon a
first plurality of encrypted data, and encrypting the second plurality of cleartext data to obtain a
second plurality of encrypted data, and wherein said cryptographic operations are performed
using cryptographic acceleration hardware.

4. (Original) The method of claim 1, wherein the at least one translation rule is
predetermined.

5. (Original) The method of claim 1, wherein the at least one translation rule is
determined dynamically.

6. (Original) The method of claim 1, wherein the first cryptographic protocol is
WTLS.

7. (Original) The method of claim 1, wherein the first plurality of encrypted data is
associated with WML.

8. (Original) The method of claim 1, wherein second plurality of encrypted data is
associated with HTML.

9. (Original) The method of claim 1, wherein the second cryptographic protocol is
SSL over HTTP.

10. (Original) The method of claim 1, wherein the first cryptographic protocol and the second cryptographic protocol are identical.

11. (Original) The method of claim 1, wherein the first plurality of encrypted data and the second plurality of encrypted data conform to different revisions of a specification for the same cryptographic protocol.

12. (Original) The system of claim 3, wherein at least one cryptographic module is a cryptographically strong pseudorandom number generator.

13. (Cancelled)

14. (Currently Amended) The system of claim ~~13~~ 3, wherein the cryptographic acceleration hardware includes a plurality of individual hardware acceleration units.

15. (Original) The system of claim 14, wherein at least one individual hardware acceleration unit is dedicated to one function.

16. (Currently Amended) The system of claim ~~13~~ 3, wherein the cryptographic acceleration hardware is updateable by loading at least one cryptographically signed instruction.

17. (Currently Amended) The system of claim ~~13~~ 3, wherein the cryptographic acceleration hardware is tamper-resistant.

18. (Currently Amended) The system of claim ~~13~~ 3, wherein the cryptographic acceleration hardware is tamper-evident.